Task 6

Hash functions have wide usage in computer science, they are often used in data structures to map certain objects into an array or another form of data structure. Using them effectively can reduce complexity to constant time. So, hash functions in general are simply functions that take arbitrary length input and give a fixed length output. A good hash function to achieve this is usually one that leads to as few collisions as possible. Collision-resistant hash functions that we use here in cryptography are similar in principle to those used in computer science, however, here collisions are not just undesirable, there strictly cannot be collisions in case of cryptography. That is, no polynomial time adversary should be able to find a distinct pair of values x and x' such that,

$$H(x) = H(x')$$

Build Algorithm

Let G be a group with generator g and order q, Then taking x1, x2 as inputs such that 0 <= x1, x2 < q

Let h be another number belonging to the group G.

Now, H_s (x1, x2) can be defined as $(g_{x1} * h_{x2}) \bmod q$.

Therefore, **$H_s (x1, x2) = g_{x1} * h_{x2}$** **___ [1]**

Proof

Assuming that discrete log problem (DLP) is hard, i.e. no polynomial time algorithm exists such that discrete log problem can be solved efficiently.

We do the proof again using proof by contradiction technique.

Let us assume that we have found a collision in $H^{s,}$ Therefore,

$$H^s (x1, x2) = H^s (x11, x22)$$

Substituting the value of H^s (x1, x2) and H^s (x11, x22) from [1], we get

$$g^{x1} * h^{x2} = g^{x11} * h^{x22}$$

Dividing both sides by $g^{x11} * h^{x2}$, we get,

$$g^{x1-x11} = h^{x22-x2}$$

Let $d = (x22 - x2)^{-1} \bmod q$

→ $$g^{(x1-x11) *d} = h^{(x22-x2) *d}$$

→ **$g^{(x1-x11) *d} = h$** **_____ [2]**

Now, it can be seen that from equation [2], we can compute h in polynomial time. However, if that is true that means that discrete log problem can also be solved in polynomial time, which we know is not the case. Therefore, we have proven that if our collision resistant hash function has collisions then discrete log problem must also be solvable by a polynomial time adversary.
Therefore, as long as dlp is hard, our function is collision resistant.